UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE RESIDENCE LOCATED AT 3956 FULTON GROVE ROAD
CINCINNATI, OHIO 45245

Case No. **1:23-MJ-00216**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252 and/or 2252A	Activities Relating to Material Involving the Sexual Exploitation of Minors

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

WESLEY DUNN Digitally signed by WESLEY DUNN Date: 2023.03.23 09:21:25 -04'00'

Applicant's signature

Wesley Dunn, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime video conference *(specify reliable electronic means)*.

Date: **Mar 23, 2023**

Stephanie K. Bowman

Judge's signature

City and state: Cincinnati, Ohio

Hon. Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

3956 Fulton Grove Rd, Cincinnati, OH 45245 (the "Premises") is a single-family home with light gray siding with white trim and a black roof. The front entryway is recessed into the center of the residence. The Premises is the third structure located on the east side of Fulton Grove Road from Ohio pike. The Premises includes all curtilage and vehicles parked on the subject Premises. The vehicle registered to Bonavita is a maroon, Honda CR-V, Ohio plate HXR8405, which may be parked in the driveway located on the left side of the residence.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. Computer(s), including cell phones, computer hardware, computer software, computer-related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, cameras, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica; and the contents therein.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including P2P software.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. Any and all visual depictions of minors, in any format and medium, including all originals, computer files, copies, and negatives, engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer at the residence located at

3956 Fulton Grove Rd, Cincinnati, **Ohio**, by use of the computer or by other means for the purpose of distributing or receiving visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) that concern any accounts with an Internet Service Provider.

7. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Any and all diaries, notebooks, notes, and any other records reflecting a person's sexual interest in minors. Any and all diaries, notebooks, notes, and any other records reflecting

personal contact or any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF THE RESIDENCE LOCATED AT 3956 FULTON GROVE ROAD, CINCINNATI, OHIO 45245	Case No. **1:23-MJ-00216** **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Wesley Dunn, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 3956 Fulton Grove Road, Cincinnati, Ohio, hereinafter "PREMISES," as further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since August 2020. I am currently assigned to the Cincinnati Division. Prior to my current position, I was employed for three years as a patrol officer for the Owensboro Police Department located in Owensboro, Kentucky. While employed by the Federal Bureau of Investigation, I have investigated federal criminal violations related to high technology or cybercrime, child pornography, identity theft, and credit card fraud. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2252 and/or 2252A have been committed by Kik user **gambit104** (believed to be Nicholas Bonavita). There is also probable cause to search the PREMISES described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

OVERVIEW OF KIK MESSENGER & THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN'S CYBERTIPLINE PROGRAM

Kik Messenger Application

5. The following information has been provided to me from the Kik Law Enforcement Guide (dated February 26, 2020), online research that I have conducted, from other law enforcement officers, as well as my training and experience. Kik Messenger, commonly called Kik, is a freeware instant messaging mobile app from the Canadian company Kik Interactive, and available free of charge on iOS and Android operating systems. It is a social networking application that permits a user to trade and disseminate various forms of digital media while using a cellphone. Kik advertised itself as "the first smartphone messenger with a built-in browser." Kik was founded in 2009 and according to its company website was designed to "break down barriers [between operating systems] that would allow users to chat with whoever, whenever." In October 2019, Kik Interactive was purchased by Santa Monica, California based MediaLab Inc. MediaLab Inc. is a holding company that owns other internet-based communication applications such as Whisper, Datpiff and others.

6. Kik Messenger is a feature within Kik that allows its users to communicate with selected persons as well as browse and share any website content with those whom the user

selects while still within the Kik platform. Unlike other messaging apps, Kik usernames – not phone numbers - are the basis for Kik user accounts. Kik usernames are unique; can never be replicated; can never be changed, may include lower and uppercase letters, numbers and/or 4 periods and underscores; and will never contain spaces, emoticons or special characters. A Kik username is the only publicly available identifier MediaLab Inc. can use to identify a Kik account to law enforcement. The company cannot identify users using phone numbers, first and last name (display name), or email address.

7. In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, sketches, stickers and even web page content by posting such content privately with individual users (with whom the user selects) or publicly (on the Kik platform) with multiple individuals who belong to "Groups." Groups are formed when like-minded individuals join collectively online in an online forum, created oftentimes by a Kik user designated as the Kik "Administrator" of the group. Groups can hold up to 50 Kik usernames. Groups are created to host/discuss topics such as modern popular culture-themed ideas as well as illicit/illegal-themed ideas. Public groups names are a user-generated hashtag; can never be replicated; can never be changed; may include lower and uppercase letters, numbers and/or periods and underscores; will never contain spaces, emoticons or special characters; The group hashtag will begin with a hash (#) (i.e.#AffidavitForWarrant).

The National Center for Missing and Exploited Children's CyberTipline Program

8. The National Center for Missing and Exploited Children (NCMEC) was incorporated in 1984 as a private, non-profit 501(c)(3) organization to serve as a national

clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited children's issues.

9. NCMEC operates the CyberTipline, a system that allows for the general public, law enforcement, private companies such as Kik, and others to report potential sexual abuse issues to NCMEC. As part of the submission process, NCMEC informs those that report that information submitted via the CyberTipline will be shared with law enforcement for possible investigation.

PROBABLE CAUSE

10. On December 13, 2022, Kik submitted a cyber-tip to the CyberTipline. Kik's cyber-tip was assigned CyberTipline report number 141507188. Report 141507188 indicated that on December 11, 2022, Kik user **gambit104** (gambit) was reported for sharing apparent child pornography. Kik conducted a review and discovered private messages sent from gambit to an unknown user. The private messages, sent on December 04, 2022 contained thirteen individual video files. A Kik employee reviewed the videos and determined them to be child pornography. The following account information was included in Kik's cyber-tip:

a. Email address: **johnmay041994@gmail.com**

b. Screen/User Name: **gambit104**

c. ESP User ID: gambit104_coo

d. IP Address: 75.185.241.70 (Login).

11. NCMEC conducted a review of the thirteen video files submitted in Kik's NCMEC cyber-tip. The review indicated that ten of the videos depicted "apparent child pornography," two were "child pornography (unconfirmed)" and one depicted an unclothed child.

12. A grand jury subpoena was served on Charter Communications Inc. to provide subscriber information pertaining to IP address 75.185.241.70 and the associated date/time when it was used to log into the gambit104 Kik account. On January 27, 2023, Charter Communications Inc. responded with the following information:

Target Details: IP 75.185.241.70

Subscriber Name: Nicholas Bonavita

Subscriber Address: 3956 Fulton Grove Rd, Cincinnati, OH 45245

Username: bbonavita62@yahoo.com, bonavita6162@charter.net

Phone Number: N/A

13. On March 13, 2023 an administrative subpoena was served on Kik Interactive for the IP address 75.185.241.70. On March 14, 2023, Kik Interactive responded with the following information:

First Name: Joe

Last Name: Bon

Account Created: 2022/11/06 21:46:06

User Location: IP: 75.185.241.70

Email: **johnmay041994@gmail.com** (unconfirmed)

Username: **gambit104**

Device Info: Nokia N152DL

14. From the response, it appears that Kik user gambit104 provided the email address johnmay041994@gmail.com during the initial registration for the account. Kik regularly uses the email address provided during registration to correspond with the registrant about their account and can be used for various functions such as conducting a password reset. The email

address, johnmay041994@gmail.com, provided by Kik is listed as unconfirmed. "Unconfirmed" means that verification link contained within the initial activation email sent by Kik to johnmay041994@gmail.com was not used. A Kik user's account being unconfirmed does not limit that user's ability to use or access Kik messenger functions.

15. An open-source database search revealed that 3956 Fulton Grove Rd, Cincinnati, Ohio 45245 is listed as Nicholas Bonavita's current residential address. Records indicate that Bonavita has lived at this address since approximately September 2021. Bonavita entered a plea of guilty to Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) in United States District Court for the Southern District of Ohio, in Case No. 1:21-cr-00124-TSB. He is currently awaiting sentencing.

16. During the month of March 2023, affiant and other law enforcement conducted physical surveillance of 3956 Fulton Grove Rd, Cincinnati, Ohio. Located in the driveway on multiple occasions was a red Honda CR-V, OH plate HRX8405, registered to Nicholas Bonavita, 3956 Fulton Grove Rd, Cincinnati, Ohio and a dark blue 2008 Chevy Malibu, OH plate JUY9799 registered to Stephen T. Simpson, 635 Carefree Drive, Cincinnati Ohio.

17. Based on surveillance of the PREMISES it appears that multiple individuals may reside in or have regular access to the PREMISES. Based on my training and experience, I know that individuals with an interest in child pornography often reoffend, which in conjunction with the subscriber information leads me to believe Bonavita may be user of the gambit104 account. Because the Kik user account can only be traced to an IP address, this application seeks to search all devices found within the PREMISES. Based on my training and experience, I know that when multiple individuals have access to an IP address, it is necessary to examine all devices located in the PREMISES in order to confirm the identity of the Kik user or users who possessed

and distributed child pornography. I also know based on my training and experience that it is not uncommon for child pornography collectors and distributors to use aliases or the names of others so a search of all devices contained within the residence is necessary for user attribution.

DEFINITIONS

18. The following definitions apply to this Affidavit and to Attachment B to this Affidavit:

a. "Child Erotica," as used herein, means materials demonstrating a sexual interest in minors, including fantasy narratives, cartoons, and books describing or alluding to sexual activity with minors, sexual aids, children's clothing catalogues, and child modeling images.

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

c. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

d. "Internet Protocol address" (or simply "IP address") is a unique numeric address used by computers on the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses

might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

e. "The Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. "Computer," as used herein, is defined pursuant to 18 U.S.C. § l030(e)(l), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

g. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be

used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. "Computer software," as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to,

microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

k. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

BACKGROUND ON COMPUTERS, CELL PHONES, AND CHILD PORNOGRAPHY

19. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, including cellphones, and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers, including cell phones, basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera

or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to anyone of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks - such as engaging in online chat, sharing digital files, reading a book, or playing a game - on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that mobile device users often connect to known wireless networks which are available to them, especially localized networks within their residence. The connection information such as usernames and passwords are typically stored within the

device and the device automatically connects when within range of a known wireless network. Individuals often set this automatic connect preference in their devices in order to conserve battery consumption, improve connection speeds, and reduce cellular data consumption which is often limited or metered. Mobile devices connected to a wireless network will often share the same IP address information as reported by the residential wireless network provider.

i. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

20. The storage capacity of the electronic storage media used in home computers and cell phones has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

21. A user can set up an online storage account from any computer or cell phone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer or cell phone. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or cell phone in most cases.

22. Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

23. Searches and seizures of evidence from cellular phones commonly require agents to download or copy information from the cellular phone to be processed later in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect

the integrity of the evidence and to recover even hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

24. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any application software that may have been used to create the data (whether stored on hard drives or on external media).

SEARCH METHODOLOGY TO BE EMPLOYED

25. The search procedure of electronic data contained in computer hardware, computer software, memory storage devices, and/or cell phones may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, memory storage devices, and/or cell phone to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality

of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B;

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

26. Most individuals who collect child pornography are sexually attracted to children, as their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences involving children. Collectors of child pornography express their attraction to children through the collection of sexually explicit materials involving children, as well as other seemingly innocuous material related to children.

27. The above-described individuals may derive sexual gratification from actual physical contact with children, as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children.

28. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica," further defined as any material relating to children that serves a sexual purpose for a given individual. "Child erotica" is broader and more encompassing than child pornography, though at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his/her intent. "Child Erotica" includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

29. Child pornography collectors often reinforce their fantasies by taking progressive, overt steps aimed at turning such fantasy(ies) into reality in some, or all, of the following ways: collecting and organizing their child-related material; masturbating while viewing child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children, thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

30. Child pornography collectors almost always maintain and possess their material(s) in the privacy and security of their homes or some other secure location, to include Internet cloud storage. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. The collector is often aroused while viewing the collection and, acting on that arousal, he/she often masturbates, thereby fueling and reinforcing his/her attraction to children.

31. Due to the fact that the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, the collector rarely disposes of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase. Individuals who use a collection in the seduction of children or to document the seduction of children treat the materials as prized possessions and are especially unlikely to part with them. Even if a child pornography collector deletes files from his hard drive or other electronic media, a computer expert is often able to retrieve those files using computer forensic tools.

CONCLUSION

32. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that Kik user gambit104, believed to be Nicholas Bonavita, who resides at the PREMISES more fully described in Attachment A, is involved in the distribution, receipt, and/or possession of child pornography, in violation of 18 U.S.C.§ 2252/2252A. Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violations of 18 U.S.C.§ 2252/2252A (distribution, receipt, and possession of child pornography), is located in the PREMISES described above, and

this evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

33. Based on the forgoing, I request that that the attached warrant be issued authorizing the search of the PREMISES described in Attachment A and seizure and search of the items listed in Attachment B.

Respectfully submitted,

WESLEY DUNN Digitally signed by WESLEY DUNN Date: 2023.03.23 09:22:57 -04'00'

Wesley Dunn
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on March 23, 2023 by reliable electronic means, specifically, FaceTime video conference.

Stephanie K. Bowman

HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

3956 Fulton Grove Rd, Cincinnati, OH 45245 (the "Premises") is a single-family home with light gray siding with white trim and a black roof. The front entryway is recessed into the center of the residence. The Premises is the third structure located on the east side of Fulton Grove Road from Ohio pike. The Premises includes all curtilage and vehicles parked on the subject Premises. The vehicle registered to Bonavita is a maroon, Honda CR-V, Ohio plate HXR8405, which may be parked in the driveway located on the left side of the residence.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

1. Computer(s), including cell phones, computer hardware, computer software, computer-related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, cameras, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica; and the contents therein.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including P2P software.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. Any and all visual depictions of minors, in any format and medium, including all originals, computer files, copies, and negatives, engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer at the residence located at

3956 Fulton Grove Rd, Cincinnati, **Ohio**, by use of the computer or by other means for the purpose of distributing or receiving visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) that concern any accounts with an Internet Service Provider.

7. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, handwritten notes, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Any and all diaries, notebooks, notes, and any other records reflecting a person's sexual interest in minors. Any and all diaries, notebooks, notes, and any other records reflecting

personal contact or any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).